USAWC STRATEGY RESEARCH PROJECT

UNSHACKLING THE SPHINX: INTELLIGENCE IN THE POST-9/11 WORLD

By

Colonel Joseph M. McNeill
United States Army

Colonel John S. Rovegno
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
18 MAR 2005		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Unshackling the Sphinx Intelligence in the Post-9/11 World	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Joseph McNeill	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**26**	

ABSTRACT

AUTHOR: Colonel Joseph M. McNeill

TITLE: UNSHACKLING THE SPHINX: INTELLIGENCE IN THE POST-9/11 WORLD

FORMAT: Strategy Research Project

DATE: 18 March 2005 PAGES: 26 CLASSIFICATION: Unclassified

The terrorist attacks on 11 September 2001 in New York, Virginia, and Pennsylvania caused an intense self-examination by the United States Federal Government in which it made tough decisions concerning the use of foreign intelligence in relation to law enforcement activities. Existing constraints to collection of foreign intelligence, dissemination to law enforcement agencies, and placement in information databases created a “wall” between the Intelligence Community and the law enforcement agencies.

Since 9/11, several key actions have worked to reduce that wall . Laws, such as the USA PATRIOT Act, the Homeland Security Act, and the Intelligence Reform and Terrorism Prevention Act have served to eliminate undue restrictions on transfer of terrorist-related intelligence between law enforcement and the Intelligence Community. Government reorganization actions led to the creation of the Department of Homeland Security, the U.S. Northern Command, and the National Counterterrorism Center, and the establishment of the new position of Director of National Intelligence.

What has not occurred, as of yet, is a review of the role Military Intelligence should have in this new construct of intelligence law and counterterrorism organization. Also, current restrictions on Military Intelligence activities within the United States can severely hamper the ability of a commander called upon to execute homeland defense or consequence management missions. A review of these restrictions is imperative. Such reviews should take place soon, in order to fully utilize the capabilities of the Military Intelligence community.

TABLE OF CONTENTS

UNSHACKLING THE SPHINX:
INTELLIGENCE IN THE POST-9/11 WORLD

> Defending our Nation against its enemies is the first and fundamental commitment of the Federal Government. Today, that task has changed dramatically. Enemies in the past needed great armies and great industrial capabilities to endanger America. Now, shadowy networks of individuals can bring great chaos and suffering to our shores for less than it costs to purchase a single tank. Terrorists are organized to penetrate open societies and to turn the power of modern technologies against us.
>
> —George W. Bush

The events of 11 September 2001 are indelibly emblazoned upon the psyche of the American people and the words of the President in his *National Security Strategy of the United States* set the tone for significant changes in the way our Federal Government views the terrorist threat. Indeed, sweeping changes in the organization of the Executive Branch as well as Congressional legislation dealing with law enforcement and intelligence activities concerning international terrorism have distinguished the first George W. Bush Administration and the 107th and 108th Congresses as almost single-mindedly focused on waging the global war on terror (GWOT).

One aspect of this 'war' that appears to be underappreciated is the role that Military Intelligence (MI) can serve the United States in defending the homeland. Military Intelligence is defined by the Department of Defense as "intelligence on any foreign military or military-related situation or activity which is significant to military policymaking or the planning and conduct of military operations and activities."[i] It can also be considered "the foreign intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps."[ii] The U.S. *Strategy for Combating Terrorism* envisions a "seamless web of defense"[iii] in the protection of the American people. However, current policy and practice limits the employment of MI in that web. The changes to government policy and law on the use of domestic and foreign intelligence since 9/11 increase the potential for the proper use of MI capabilities in support of domestic security. However, to date, the changes that have been put in effect do not directly enable MI to provide that support.

Following a brief description of two key national strategies affecting terrorism and homeland security, each of which place value in the contributions intelligence can provide, this paper will analyze the conditions pertaining to intelligence sharing and law enforcement leading to the events of 9/11 and the federal government's responses to improve such intelligence sharing. It will conclude with a summary of key actions necessary for MI to properly integrate into the United States' 'seamless web of defense.'

STRATEGIC CONCEPTS

The United States elevated the defeat of global terrorism as a key concept in the attainment of its goals as outlined in its *National Security Strategy*.[iv] To that end, the Bush Administration developed several supporting strategies which heretofore had not enjoyed the status of 'national strategies.' Two key documents in this hierarchy of strategies are the *National Strategy for Combating Terrorism* , focusing "on identifying and detecting threats before they reach our borders,"[v] and the *National Strategy for Homeland Security*, which "focuses on preventing terrorist attacks within the United States."[vi] Together, these strategies establish a framework with which to array the ends, ways, and means necessary to protect the United States from the effects of global terrorism.

NATIONAL STRATEGY FOR COMBATING TERRORISM

The *National Strategy for Combating Terrorism* identifies the attainment of four goals as essential for success:

- "defeat terrorists and their organizations;"
- "deny sponsorship, support, and sanctuary to terrorists;"
- "diminish the underlying conditions that terrorists seek to exploit;" and,
- "defend U.S. citizens and interests at home and abroad."[vii]

This *defeat*, *deny*, *diminish*, *defend* strategy envisions the employment of all instruments of national power – "diplomatic, economic, law enforcement, financial, information, intelligence, and military" in achieving these goals.[viii]

Although no one goal has primacy on any other, U.S. strategy establishes the priorities of defeating and defending. "Our priority will be first to disrupt and destroy terrorist organizations of global reach and attack their leadership; command, control, and communications; material support; and finances. This will have a disabling effect upon the terrorists' ability to plan and operate."[ix] Further, "we will defend the United States, our citizens, and our interests at home and abroad…"[x] Key resources for executing these priorities include the Intelligence Community and law enforcement agencies,[xi] as well as the military. [xii]

What will become critical to success as the nation mobilizes to fight the war on terror is the level of integration of these key resources. As will be addressed later, there have been and continue to be in place some policies designed to protect individual liberties which, in effect, limit true integration. While the policies serve to provide checks and balances on our law enforcement activities, they have been perceived to create significant barriers to effective execution of the counterterrorism effort.

NATIONAL STRATEGY FOR HOMELAND SECURITY

Within a month of 9/11, President Bush created the Office of Homeland Security within the White House. He then directed it to create the first ever *Strategy for Homeland Security*[xiii] in order to coordinate the critical principles, ideas, efforts, and resources toward protecting the homeland. The strategy identified three objectives:

- "prevent terrorist attacks within the United States;
- reduce America's vulnerability to terrorism; and
- minimize the damage and recover from attacks that do occur."[xiv]

It further identifies six critical mission areas:

- "intelligence and warning;
- border and transportation security;
- domestic counterterrorism;
- protecting critical infrastructure and key assets;
- defending against catastrophic terrorism; and
- emergency preparedness and response."

Of these six areas, the first three are oriented primarily to preventing terrorist attacks.[xv]

The *Strategy* further identifies four *foundations* - law, science and technology, information sharing and systems, and international cooperation - upon which to evaluate the effectiveness of homeland security resources.[xvi] Of particular interest to this research effort are law and information sharing.

The *Strategy* relies heavily on an intelligence and warning system which can determine terrorist activity before it becomes an attack on the U.S.[xvii] The environment that characterizes the United States - large, diverse, mobile, open, with emphasis on civil liberties - enables terrorists to operate and move freely within its boundaries. For that reason, intelligence indicators are often vague and ambiguous.[xviii] Yet, "[a]ctionable intelligence is essential for preventing acts of terrorism."[xix] And, adequate warning is essential to allow governments, first responders, and the citizenry to take appropriate action.[xx]

Each of the critical mission areas is clearly interconnected and, thus, shares the challenge presented earlier concerning true integration of resources – most importantly, information. The *Strategy* identifies the challenge of information sharing quite plainly, "[o]ur current shortcoming in this area stems, in part, from the number of laws, regulations, and guidelines controlling intelligence operations."[xxi]

LIMITATIONS ON THE USE OF INTELLIGENCE

Because the demands of national security and personal privacy can be extremely competitive, the Congress and President each addressed the use of intelligence – Congress with the enactment of the *Foreign Intelligence Surveillance Act of 1978* (FISA) and President Ronald Reagan with issuance of Executive Order (EO) 12333, *United States Intelligence Activities* in 1981. Each established the provisions under which lawful collection and dissemination of intelligence information concerning United States persons could be conducted, and accordingly, identified safeguards for personal privacy. EO 12333 defines "United States person" as

> … a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.[xxii]

A brief summary of FISA and EO 12333 follows:

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

The FISA established a "statutory framework for the use of electronic surveillance" (and, with subsequent legislation, other means of collection) "in the context of foreign intelligence gathering."[xxiii] The basic idea of the law is to separate criminal activity from the activities of foreign governments. Therefore, the conventional notion of probable cause, as in a criminal case, is not wholly applicable in a foreign intelligence case.[xxiv]

However, the Act provides safeguards on the rights of individuals through the establishment of a Foreign Intelligence Surveillance Court which grants electronic surveillance orders and a Court of Review which reviews denials of such grants.[xxv] The law also establishes the principle of minimization, which restricts the acquisition, retention, and dissemination of 'nonpublicly available information' about United States persons to certain conditions, including the role of that information in foreign intelligence processes or the threat of death or serious injury to any person.[xxvi] Thus, FISA provides the ability to collect foreign intelligence information within the United States, while at the same time establishing conditions by which individual rights are maintained.

PRESIDENTIAL EXECUTIVE ORDER 12333

Partly as a result of abuses committed by MI and Counterintelligence activities during the Civil Rights and anti-Viet Nam War demonstration era of the 1960s and early 1970s, President Ford signed an EO placing strict controls on intelligence activities in 1976. Subsequently, President Carter signed his own version. Then, on 4 December 1981, President Reagan signed the current EO 12333, *United States Intelligence Activities*, replacing the Ford and Carter versions. The intent was to regulate intelligence collection, retention and dissemination activities and to establish an oversight process in order to maintain the balance between intelligence requirements and individual rights.[xxvii] "Set forth below…are certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and the protection of individual interests."[xxviii]

The order assigns to the Intelligence Community the responsibility to collect, produce, and disseminate intelligence for the purpose of protecting national security, as well as countering international narcotics and terrorist activities.[xxix] The order also constrains collection activities concerning United States persons, assigning responsibility for such collection to the Federal Bureau of Investigation.[xxx] However, it acknowledges that at times it may be more suitable for others in the Intelligence Community to conduct the collection activity.

In all cases, intelligence collection against United States persons, including "electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices,"[xxxi] "for which a warrant would be required if undertaken for law enforcement purposes," must be approved by the Attorney General, based upon his/her determination of probable cause that the collection is conducted against a foreign power or an agent of a foreign power.[xxxii]

Finally, the order directed that the Defense Secretary, Director of Central Intelligence, Attorney General, and National Security Council publish the necessary directives in order to implement the order.[xxxiii]

DEPARTMENT OF DEFENSE IMPLEMENTATION

Pursuant to EO 12333, the Secretary of Defense issued Department of Defense (DOD) Directive 5240.1, and subsequently its guiding regulation, DOD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*. Each service published its own supporting regulation, implementing the procedures within EO 12333 and DOD 5240.1-R. For simplicity, the governing Department of the Army (DA) regulation, Army Regulation (AR) 381-10, *US Army Intelligence Activities*, which closely follows the DOD regulation, will be used to expand upon the

DOD implementation of EO 12333. The regulation stipulates fifteen procedures, the first procedure administratively governing the general aspects of the program. Procedures Two through Four establish the authority for collection, retention, and dissemination of information concerning United States persons. Procedures Five through Ten govern the collection techniques - electronic surveillance, concealed monitoring, physical search, mail surveillance, or physical surveillance - which may be employed by intelligence or counterintelligence personnel. And finally, Procedures Eleven through Fifteen control other aspects of collection activity, to include intelligence oversight.[xxxiv]

Consistent with FISA and EO 12333, MI personnel may collect foreign intelligence information on a U.S. person if the target is "reasonably believed" to be an agent of a foreign power or if the person is "engaged or about to be engaged in international terrorist or international narcotics activities."[xxxv] However, such collection has to meet several conditions, including a test of significance and exclusivity - meaning it is not concerning domestic activity of the target, overt methods are not appropriate, coordination is affected with the Federal Bureau of Investigation (FBI), and there is written authorization by the designated DA authority. The designated authorities within DA are the Army G2 and the Commander, Intelligence and Security Command.[xxxvi] These conditions serve to constructively constrain collection activities in order to ensure the Secretary of Defense meets his obligations to EO 12333 and the Attorney General.

PRIVACY VERSUS SECURITY

The foregoing has been a brief treatment of the statutory and regulatory controls from Congress and the President down to Service Department level on collection of intelligence information that were in place at the time of the terrorist attacks on 11 September 2001. The struggle to maintain balance between national security and individual rights emanates from the Fourth Amendment to *The Constitution of the United States*:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[xxxvii]

Two basic concepts germane to the issue of intelligence collection arise from analysis of the 4th Amendment. First, the amendment is designed to protect the law abiding citizen, not the criminal. After establishment of probable cause, the target of the collection (search) is subject to any search which can give evidence. Where probable cause is not established, those U.S. persons are shielded from

search.[xxxviii] The second concept is the existence of a system of checks and balances in the process of allowing the search. Even the most well-intentioned investigator can be subject to the passion of the search for evidence, such that he loses objectivity in establishing the existence of probable cause. For this reason, the judiciary possesses the authority to issue warrants and appropriately scope the search before it occurs.[xxxix]

The processes internal to the requirements laid out in FISA and EO 12333 adequately incorporate these concepts. However, as an unintended consequence, the provisions create a natural conflict between the law enforcement agencies of the federal government and the Intelligence Community. What is important to understand about the effect of these regulations is the effect their implementation has had on sharing intelligence information with law enforcement and the subsequent effect on the United States' counterterrorism efforts. Each has its own purposes for acquisition of the information. In law enforcement, the aim is generally criminal prosecution, and therefore the information is collected with full intention of disclosure to the accused. In the Intelligence Community, however, which is focused on protection of national security from forces hostile to the United States, oftentimes information comes by way of sources and methods the Intelligence Community would rather not announce to the terrorist entity that are being utilized. These divergent perspectives on the purposes of information and intelligence especially clash in the realm of international terrorism, since such activity has both a criminal and a national security component.[xl]

The central tendency to separate intelligence from law enforcement investigative information was exacerbated by interpretation of the law. Specifically, the FBI became convinced, as an institution, that it could not pass any intelligence information, whether produced using FISA techniques or not, to criminal investigators.[xli] The tension between privacy and security manifest itself as a very real set of barriers between the two entities fighting terrorism. The 9/11 Commission popularized the term for the collective effect of these barriers as 'the wall.'[xlii]

SIGNIFICANT ACTIONS SINCE 9/11

September 11 was a call to arms, literally and figuratively, across all sectors of the federal government. Some action was swift, ranging from the military response in Afghanistan and passage of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act* to reorganizing the federal government by creating the Department of Homeland Security. Other actions have taken longer, and include intelligence reform and the establishment of the National Counterterrorism Center. Much of the focus of the post-9/11 energy has been on how to prevent the glaring oversights leading to that tragic day.

KEY 9/11 COMMISSION OBSERVATIONS AND RECOMMENDATIONS

Amidst the urgency to put in place the changes necessary to protect the United States from future attacks, it must have become clear to the national leaders that they had not quite scoped the extent of the problem. While certain changes may have seemed obvious, at issue was the fundamental question of how the country exposed its flank in the first place. In order to effect an objective, nonpartisan investigation, Congress and the President, through Public Law 107-306, 27 November 2002, created the National Commission on Terrorist Attacks Upon the United States. This Commission is known today by the more familiar sobriquet, '9/11 Commission.'[xliii]

While the 9/11 Commission delved into a broad array of government operations in order to determine the root causes for America's guard to be down, of particular import to this research effort is the role of intelligence. The Commission, as noted earlier, diagnosed the barriers between foreign intelligence and domestic information. One of its key observations concerned the relationship between foreign intelligence collection and that collection's purpose.

> In addition to requiring court review of proposed surveillance (and later, physical searches), the 1978 Act was interpreted by the courts to require that a search be approved only if its 'primary purpose' was to obtain foreign intelligence information. In other words, the authorities of the FISA law could not be used to circumvent traditional criminal warrant requirements.[xliv]

The Office of Intelligence Policy and Review (OIPR) of the Department of Justice, which handles FISA applications before the FISA Court, determined, based upon its own interpretations of FISA, that the exchange between FBI agents and prosecutors might be construed by the Court as improper use of the warrant. Put more plainly, it felt that the Court might perceive a law enforcement 'angle' on a FISA application. At the time, the Aldrich Ames espionage investigation was in full swing and the Justice Department did not want to destroy the case. The OIPR interpretation and subsequent strict procedures remained in effect through 9/11.[xlv]

The National Security Agency (NSA) also faced challenges with collection and dissemination of intelligence. Since FISA prohibits the agency from deliberately collecting data on U.S. persons, it took on a culture of avoiding anything domestic, even if technically and lawfully able to collect the information.[xlvi] Restrictions to mixing domestic information with foreign intelligence, established by EO, also contributed to the agency's inability to transfer intelligence to law enforcement. The 9/11 Commission observed that the NSA had intelligence reports about Usama bin-Laden, but because of its handling procedures, this information either did not get to the FBI or it arrived in such a manner as to be untimely or ill-understood.[xlvii]

In addition to many other failures within the government, the 9/11 Commission observed that the Intelligence Community suffered from both real and perceived barriers to the effective handling of intelligence information pertaining to the events leading to the terrorist attacks on September 11. This intelligence failure formed the basis of three of the five major recommendations developed in their report. These three recommendations are:

- "unifying strategic intelligence and operational planning against Islamist terrorists across the foreign-domestic divide with a National Counterterrorism Center;"
- "unifying the intelligence community with a new National Intelligence Director;" and,
- "unifying the many participants in the counterterrorism effort and their knowledge in a network-based information-sharing system that transcends traditional governmental boundaries."[xlviii]

The essence of their findings is that, although proper rules exist in order to protect individual liberties, governmental culture and bureaucracy have grossly misrepresented those protections and created an environment devoid of a synoptic view of the battlespace (i.e. – the U.S. homeland). The 'stovepipes' hindered any one agency from seeing enough information to detect, identify, classify, and neutralize the threat. Hence, in the commission's collective judgment, some form of governmental reorganization is in order to break down the 'walls' and unify the efforts of thousands of people, all doing the right things but to a detrimental, or at least suboptimal, effect.

FEDERAL RESPONSES

Even while the 9/11 Commission was conducting its inquiry, the federal government was in the midst of significant change, both physically and philosophically, to deal with the threat of international terrorism. Congress had already passed the *USA PATRIOT Act* and was tackling the issue of intelligence reform. The Executive Branch had reorganized, first creating the Office of Homeland Security, and then, subsequent to Congressional legislation, the Department of Homeland Security. The *National Security Strategy* characterized this reorganization as "the largest government reorganization since the Truman Administration created the National Security Council and the Department of Defense."[xlix] Philosophically, the *Strategy for Homeland Security* recognized that "Congress, with the enactment of the *USA PATRIOT Act*, took important steps toward identifying and removing some barriers to the exchange of intelligence."[l] More steps were to come. The following is a brief analysis of the significant activities at the federal level which impact upon the use of intelligence.

USA PATRIOT ACT

The *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act* was a watershed event in the federal government's approach to intelligence and terrorism. Rapidly developed and, some say, rammed through Congress,[li] the Act eased restrictions on intelligence collection and enabled interaction between the Intelligence Community and law enforcement agencies. One particular point of import is that the Act allowed applications for FISA collection to be contingent upon foreign intelligence as a *significant* reason for collection, as opposed to *the* reason (emphasis added) for collection,[lii] accounting for the recognition that investigations of criminal activity and international terrorism may overlap.

> The Act removed the major legal barriers that prevented law enforcement, intelligence, and national defense communities from talking and coordinating their work to protect the American people and our national security. The government's prevention efforts should not be restricted by boxes on an organizational chart. Now police officers, Federal Bureau of Investigation agents, Federal prosecutors, and intelligence officials can protect our communities by "connecting the dots" to uncover terrorist plots before they are completed.[liii]

While the counterargument has been that, in effect, the Act significantly lessens the role of the impartial judicial branch in the system of checks and balances on national security versus civil liberties,[liv] the prevailing sentiment, as characterized above by the 9/11 Commission, is that the Act goes a long way to removing the unduly strict interpretations of the FISA law.

Government Reorganization

President Bush established the Office of Homeland Security (OHS) by EO on 8 October 2001. The OHS was tasked to "coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States."[lv] Although initial efforts were laudable, it became clear that an office internal to the Executive Office of the White House could not adequately execute the tasks. With passage of the *Homeland Security Act of 2002* , Congress and the President created the Department of Homeland Security (DHS), moving several agencies and bureaus from other departments and placing them in the DHS. The department's primary mission is to prevent terrorist attacks, reduce vulnerability, and minimize damage in the event of terrorist attacks within the United States.[lvi]

These efforts did not get to the heart of the issue, as seen by the 9/11 Commission and others - that of intelligence. The need was for an entity with access to all-source intelligence, foreign and domestic, with which it could fuse, analyze, and produce a more complete terrorism intelligence picture.[lvii] The

9/11 Commission called for creation of a "trusted information network."[lviii] The existing bureaucratic, legal, and human resistance to sharing information[lix] was an impediment to getting the intelligence out of the community and into the hands of those assessing threats to our national security. [lx] The *Homeland Security Act* specifically addressed the issue of the "wall" by allowing, by amendment to the FISA, the interaction between law enforcement and the FISA intelligence collectors.[lxi] But this action is limited in its effectiveness because, while extremely useful for a particular case, it does not contribute to the greater "trusted information network."

On 27 August 2004, the President established by Executive Order the National Counterterrorism Center (NCC) to be the organization which would analyze and integrate terrorism-related intelligence.[lxii] He directed all agency heads to ensure such information was made available to the Director of the Center.[lxiii] Subsequently, the *Intelligence Reform and Terrorism Prevention Act of 2004* provided statutory authority for the NCC.[lxiv] Through these actions, the federal government established a mechanism to break down the "wall" and fuse terrorism-related intelligence from virtually all sources.

Another significant organizational decision made by the President was the designation of a military combatant command, the United States Northern Command (NORTHCOM), whose mission is homeland defense and civil support. Its purpose is to deter, prevent, and defeat threats to the United States, and assist in consequence management.[lxv] As a joint force commander (JFC), the commander of NORTHCOM exercises command authority over forces assigned to him for either of these missions. As with all commanders, intelligence is a crucial tool in his ability to lead his force and execute his mission. Intelligence is absolutely vital in enabling the JFC to visualize his battlespace and understand his enemy.[lxvi] The extant statutes and regulations limit the ability of MI organizations, in effect the only organic intelligence organizations available to the commander, from providing that vital intelligence information. NORTHCOM is almost exclusively a consumer of products, generally tailored for Administration policy-makers, from the national and DOD intelligence agencies. To the extent that NORTHCOM does not routinely need to execute tactical missions, this constraint may have minimal effect on operations. However, in the event NORTHCOM is called upon to execute a homeland defense mission concerning some form of terrorist activity, tactical level intelligence collected within the United States by MI organizations will be critical.

Intelligence Reform and Terrorism Prevention Act of 2004

The latest in the federal actions to confront the failings of the government to prevent the attacks on 9/11 is the passage of the *Intelligence Reform and Terrorism Prevention Act of 2004* . Attempting to unify the federal counterterrorism effort, and at the suggestion of the 9/11 Commission, Congress

established a Director of National Intelligence to lead the Intelligence Community, establish and prioritize foreign intelligence requirements, and assist the Attorney General in disseminating FISA-related intelligence.[lxvii] As mentioned above, it also established the National Counterterrorism Center. Strengthening the federal commitment to better information sharing, and again at the urging of the 9/11 Commission, the Act also directs the President to establish a secure Information Sharing Environment.[lxviii]

Quite plainly, through the above actions, the Federal Government has undertaken aggressive steps to refine an incredibly capable intelligence system in order to allow it to better serve the American people. Its focus in these actions has been on enabling the intelligence system to cross the imaginary yet very real boundary between foreign and domestic intelligence as it pertains to defending the homeland from terrorist attacks.

"CONNECTING THE DOTS"

In the words of the 9/11 Commission:

> As presently configured, the national security institutions of the U.S. government are still the institutions constructed to win the Cold War. The United States confronts a very different world today. Instead of facing a few very dangerous adversaries, the United States confronts a number of less visible challenges that surpass the boundaries of traditional nation-states and call for quick, imaginative, and agile responses.[lxix]

That agility is fueled by understanding. The ability of the 'national security institutions' to understand the threats facing the United States directly contributes to their ability to neutralize those threats. Understanding arises from the ability to see the threat and know the adversary's intentions. The *Strategy for Combating Terrorism* describes the notion of understanding in terms of "domain awareness", "the effective knowledge of all activities, events, and trends within any specified domain (air, land, sea, cyber) that could threaten the safety, security, or environment of the United States or its populace."[lxx] Agility stems from that understanding being timely and accurate.

Given the nature of the threat of international terrorism, that it transcends the classic lines of criminal and foreign agent/government, Congress and the President have accepted that the two types of information may be inter-related and have changed the nature of how they can be used. However, while President Bush recognizes the need to employ every "tool in our arsenal,"[lxxi] the federal government has yet to address the appropriate role of the military, and by extension, MI, to act within the United States.[lxxii]

This can be rectified in two ways. First, the President, through his Director of National Intelligence and Secretary of Defense, should review of the military's role in the GWOT. This review should include examination of and necessary modifications to EO 12333 and DOD's implementing directive, DODD 5240.1. This review should include an assessment of current and projected MI collection, processing, and dissemination capabilities and should be informed by the results of MI activity in U.S. operations in, at least, the Balkans, Afghanistan, and Iraq.

While MI activities are focused on the operational and tactical requirements of the Joint Force Commander and his subordinates, the type and value of intelligence gathered do not adhere strictly to those categories. Hence, some gathered intelligence will have exceptional value to key decision-makers involved in the counterterrorism effort back in the United States. The review of procedures should consider that possibility and devise an efficient process, using the envisioned 'Information Sharing Environment,' to get that perishable intelligence to the National Counterterrorism Center. The process must incorporate any decisions made about Judge Advocate General and Attorney General reviews, and should also consider, as an option, after-the-fact review in order to speed the process.

Second, the Secretary of Defense, in conjunction with the Secretary of Homeland Defens e, the Attorney General, and the Director of National Intelligence, should review the roles and missions of NORTHCOM and the extant limitations it has in intelligence operations. Consideration must be given to the nature of the command, in that it does not have assigned forces and by default any forces subsequently assigned to meet a crisis will have little or no situational awareness at the tactical level. The commander on the ground must have available to him, even in the role of supporting another agency, as much intelligence as possible concerning the physical, cyber, and threat environments. For that reason, the commander must not be restrained from utilizing organic intelligence gathering assets if they are appropriate to the environment. The commander on the ground must have available to him clear and concise intelligence 'rules of engagement' which have been vetted by Judge Advocate and approved by the Combatant Commander.

The Intelligence staff of NORTHCOM should be integrated into the 'Information Sharing Environment' and should be a client of the NCC from the outset. This capability, in keeping with any constraints and restraints determined to be necessary in order to protect the privacy of citizens, is essential in order to rapidly integrate any forces assigned to the command to execute a homeland defense or consequence management mission. Without it, the onset of any crisis will be characterized by an ill-informed and therefore ill-defined military capability which, presumably, must be able to execute any mission on extremely short notice.

These two recommendations are paradigm-breakers in a time of broken paradigms. That is, they are not out of line with the philosophy that has been fostered by Congress and the President since 9/11. Intelligence is vital to understanding. It is vital to the United States' ability to protect its territory from hostile acts by a foreign power or an international terrorist group. What the nation discovered about itself is that, over time, the balance between national security and personal privacy became uneven. National security lost. "The existing boundaries to intelligence sharing exist for a reason, but they must not become an excuse for bureaucratic inertia…"[lxxiii] The challenge of overcoming Cold War thinking in the 21st century includes the challenge of overcoming bureaucratic inertia. MI can provide tremendous capability to the national effort in countering terrorism, but it is burdened by bonds of restraint. In order for the nation to reap the benefits of its capabilities, the restraints must be loosened.

WORD COUNT = 5378

ENDNOTES

[i] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Pub 1-02 (Washington, D.C.: U.S. Joint Chiefs of Staff, 9 June 2004), 333.

[ii] Ronald W. Reagan, *United States Intelligence Activities*, Executive Order 12333 (Washington, D.C.: The White House, 4 December 1981), sec 1.12; available from <http://www.reagan.utexas.edu/resource/speeches/1981/120481d.htm>; Internet; accessed 12 November 2004.

[iii] George W. Bush, *National Strategy for Combating Terrorism* (Washington, D.C.: The White House, February 2003), 25.

[iv] George W. Bush, *The National Security Strategy of the United States of America* (Washington, D.C.: The White House, September 2002), 1.

[v] Bush, *Strategy for Combating Terrorism* , 2.

[vi] Ibid.

[vii] Ibid., 15, 17, 22, 24.

[viii] Ibid., 1.

[ix] Bush, *National Security Strategy*, 5.

[x] Bush, *Strategy for Combating Terrorism* , 12.

[xi] Ibid., 16.

[xii] Ibid., 17.

[xiii] U.S. Office of Homeland Security, *National Strategy for Homeland Security* (Washington, D.C.: The White House, July 2002), iii.

[xiv] Ibid., 3.

[xv] Ibid., 4.

[xvi] Ibid.

[xvii] Ibid., 15.

[xviii] Ibid., 15-16.

[xix] Ibid., 16.

[xx] Ibid., 17.

[xxi] Ibid., 48.

[xxii] Reagan, sec 3.4(i).

[xxiii] Elizabeth B. Bazan, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions* (Washington, D.C.: Congressional Research Service, 22 September 2004), ii; available from <https://www.us.army.mil/suite/doc/1337672>; Internet; accessed 8 November 2004.

[xxiv] Stephen J. Schulhofer, *The Enemy Within: Intelligence Gathering, Law Enforcement, and Civil Liberties in the Wake of September 11* (New York: The Century Foundation Press, 2002), 38.

[xxv] *Foreign Intelligence Surveillance Act, U.S. Code*, vol. 50, sec. 1803(a) (1978); available from <http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t49t50+1773+0++%28Foreign%20Intelligence%20Surveillance%20Act%29%20%20AND%20%28%2850%29%20ADJ%20USC%29%3ACITE%20AND%20%28USC%20w%2F10%20%281801%29%29%3ACITE%20%20%20%20%20%20%20%20%20>; Internet; accessed 18 January 2005.

[xxvi] Ibid., sec. 1801(h).

[xxvii] Assistant to the Secretary of Defense (Intelligence Oversight), "Mission and History;" available from <http://www.dod.mil/atsdio/mission.html>; Internet; accessed 20 January 2005.

[xxviii] Reagan, sec. 2.2.

[xxix] Ibid., sec. 1.4.

[xxx] Ibid., sec. 2.3.

[xxxi] Ibid., sec. 2.4.

[xxxii] Ibid., sec. 2.5.

[xxxiii] Ibid., sec. 3.2.

[xxxiv] U.S. Department of the Army, *U.S. Army Intelligence Activities*, Army Regulation 381-10 (Washington, D.C.: U.S. Department of the Army, 1 July 1984), 1.

[xxxv] Ibid., 2.

[xxxvi] Ibid., 3.

[xxxvii] U.S. Government Printing Office, *The Constitution of the United States* (Washington, D.C.: Government Printing Office, 2000), 4th Amendment.

[xxxviii] Schulhofer, 34.

[xxxix] Ibid., 35.

[xl] Dana R. Dillon, "Breaking Down Intelligence barriers for Homeland Security," *The Heritage Foundation Backgrounder*, no. 1536 (15 April 2002); available from <http://www.heritage.org/library/backgrounder/bg1536.html>; Internet; accessed 10 January 2005.

[xli] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton, 2004), 79.

[xlii] Ibid.

[xliii] Ibid., xv.

[xliv] Ibid., 78.

[xlv] Ibid.

[xlvi] Ibid., 87.

[xlvii] Ibid., 80.

[xlviii] Ibid., 399-400.

[xlix] Bush, *National Security Strategy*, 6.

[l] Office of Homeland Security, 48.

[li] The Congressional Digest Corporation, "Opposing Viewpoint – Analysis by the Center for Democracy and Technology," *Congressional Digest* (November 2004), 264.

[lii] The Congressional Digest Corporation, "PATRIOT Act Overview – Major Provisions and the Library Controversy," *Congressional Digest* (November 2004), 259.

[liii] The Congressional Digest Corporation, "Administration Position – Justice Department Examination of the PATRIOT Act," *Congressional Digest* (November 2004), 263.

[liv] Schulhofer, 4.

[lv] George W. Bush, *Establishing the Office of Homeland Security and the Homeland Security Council*, Executive Order 13228 (Washington, D.C.: The White House, 8 October 2001), sec. 3; available from <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=fr10oc01-144.pdf>; Internet; accessed 25 January 2005.

[lvi] *Homeland Security Act, U.S. Code*, vol. 6, sec. 101 (2002); available from <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?bdname=107_cong_public_laws&docid=f:public296.107.pdf>; Internet; accessed 25 January 2005.

[lvii] Dillon, 2.

[lviii] National Commission on Terrorist Attacks, 418.

[lix] Ibid., 416.

[lx] Dillon, 1.

[lxi] Bazan, CRS-84.

[lxii] George W. Bush, *National Counterterrorism Center*, Executive Order 13354 (Washington, D.C.: The White House, 27 August 2004), sec. 3; available from <http://a257.g.akamaitech.net/7/257/2422/06jun20041800/edocket.access.gpo.gov/2004/pdf/04-20050.pdf>; Internet; accessed 8 January 2005.

[lxiii] Ibid., sec. 6.

[lxiv] *Intelligence Reform and Terrorism Prevention Act of 2004*, "Bill Summary and Status" (17 December 2004), sec. 1021; available from <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:SN02845:@@@D&summ2=m&>; Internet; accessed 23 January 2005.

[lxv] U.S. Northern Command, "Who We Are – Mission;" available from <http://www.northcom.mil/index.cfm?fuseaction=s.who_mission>; Internet; accessed 15 January 2005.

[lxvi] U.S. Joint Chiefs of Staff, *Doctrine for Intelligence Support to Joint Operations*, Joint Pub 2-0 (Washington, D.C.: U.S. Joint Chiefs of Staff, 9 March 2000), I-1.

[lxvii] *Intelligence Reform and Terrorism Prevention Act of 2004*, sec. 104.

[lxviii] Ibid., sec. 1016.

[lxix] National Commission on Terrorist Attacks, 399.

[lxx] Bush, *Strategy for Combating Terrorism* , 25.

[lxxi] Bush, *National Security Strategy*, iii.

[lxxii] Office of Homeland Security, 48.

[lxxiii] Dillon, 4.

BIBLIOGRAPHY

Assistant to the Secretary of Defense (Intelligence Oversight). "Mission and History." Available from <http://www.dod.mil/atsdio/mission.html>. Internet. Accessed 20 January 2005.

Bazan, Elizabeth B. *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and recent Judicial Decisions*. Washington, D.C.: Congressional Research Service, 22 September 2004. Available from <https://us.army.mil/suite/doc/1337672>. Internet. Accessed 8 November 2004.

Bush, George W. *Establishing the Office of Homeland Security and the Homeland Security Council* . Executive Order 13228. Washington, D.C.: The White House, 8 October 2001. Available from<http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=fr10oc01-144.pdf>. Internet. Accessed 25 January 2005.

_____. *National Counterterrorism Center*. Executive Order 13354. Washington, D.C.: The White House, 27 August 2004. Available from <http://a257.g.akamaitech.net/7/257/2422/06jun20041800/edocket.access.gpo.gov/2004/pdf/04-20050.pdf>. Internet. Accessed 8 January 2005.

_____. *The National Security Strategy of the United States of America*. Washington, D.C.: The White House, September 2002.

_____. *National Strategy for Combating Terrorism* . Washington, D.C.: The White House, February 2003.

The Congressional Digest Corporation. "Administration Position – Justice Department Explanation of the PATRIOT Act." *Congressional Digest* (November 2004): 262-263.

_____. "Opposing Viewpoint – Analysis by the Center for Democracy and Technology." *Congressional Digest* (November 2004): 264-265.

_____. "PATRIOT Act Overview – Major Provisions and the Library Controversy." *Congressional Digest* (November 2004): 258-261.

Dillon, Dana R. "Breaking Down Intelligence Barriers for Homeland Security." *The Heritage Foundation Backgrounder*, No. 1536 (15 April 2002): 1-6. Available from <http://www.heritage.org/library/backgrounder/bg1536.html>. Internet. Accessed 10 January 2005.

Foreign Intelligence Surveillance Act. U.S.Code. Vol. 50, secs . 1801-62 (1978). Available from <http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t49t50+1773+0++%28Foreign%20Intelligence%20Surveillance%20Act%29%20%20AND%20%28%2850%29%20ADJ%20USC%29%3AC ITE%20AND%20%28USC%20w%2F10%20%281801%29%29%3ACITE%20%20%20%20%20%20%20%20%20 >. Internet. Accessed 18 January 2005.

Homeland Security Act. U.S. Code. Vol. 6, sec. 101 (2002). Available from <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?bdname=107_cong_public_laws&docid=f:public296.107.pdf >. Internet. Accessed 25 January 2005.

Intelligence Reform and Terrorism Prevention Act of 2004 . "Bill Summary and Status." 17 December 2004. Available from <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:SN02845:@@@D&summ2=m&>. Internet. Accessed 23 January 2005.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*. New York: W.W. Norton, 2004.

Reagan, Ronald W. *United States Intelligence Activities*. Executive Order 12333. Washington, D.C.: The White House, 4 December 1981. Available from <http://www.reagan.utexas.edu/resource/speeches/1981/120481dhtm>. Accessed 12 November 2004.

Schulhofer, Stephen J. *The Enemy Within: Intelligence Gathering, Law Enforcement, and Civil Liberties in the Wake of September 11* . New York: the Century Foundation Press, 2002.

U.S. Department of the Army. *U.S. Army Intelligence Activities*. Army Regulation 381-10. Washington, D.C.: U.S. Department of the Army, 1 July 1984.

U.S. Government Printing Office. *The Constitution of the United States*. Washington, D.C.: Government Printing Office, 2000.

U.S. Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms*. Joint Pub 1-02. Washington, D.C.: U.S. Joint Chiefs of Staff, 9 June 2004.

_____. *Doctrine for Intelligence Support to Joint Operations*. Joint Pub 2-0. Washington, D.C.: U.S. Joint Chiefs of Staff, 9 March 2000.

U.S. Northern Command. "Who We Are – Mission." Available from <http://www.northcom.mil/index.cfm?fuseaction=s.who_mission>. Internet. Accessed 15 January 2005.

U.S. Office of Homeland Security. *National Strategy for Homeland Security*. Washington, D.C.: The White House, July 2002.